CLAIMS

What is claimed is:

1. A data switching device for connecting to a series of nodes and to a first fabric, the device comprising:

a plurality of fabric ports for connecting to the series of nodes and forming a second fabric;

at least one node port for connecting to the first fabric; and

a switch coupled to said plurality of fabric ports and said at least one node port for interconnecting said ports.

2. The device of claim 1, wherein said at least one node port operates as a virtual node port, with one virtual node address for each of said plurality of fabric ports connected to nodes.

3. The device of claim 1, wherein said switch is further adapted to act as a firewall.

4. The device of claim 1, wherein said switch is further adapted for intrusion detection.

5. The device of claim 1, further comprising:

at least one intermediate port coupled to said switch, wherein said switch routes frames between said plurality of fabric ports and said at least one node port through said at least one intermediate port.

6. The device of claim 5, wherein the interconnection between said at least one intermediate port and either said plurality of fabrics ports or said at least one node port is a private interconnection and said at least one intermediate port and said other port perform public to private and private to public address translations.

7. The device of claim 5, wherein the number of intermediate ports equals the number of node ports.

8. The device of claim 1, wherein said switch performs public to private and private to public address translations between said plurality of fabric ports and said at least one node port.

9. A Fibre channel switch for connecting to a series of nodes and to a first fabric, the switch comprising:

a plurality of F_ports for connecting to the series of nodes and forming a second fabric;

at least one N_port for connecting to the first fabric; and

a switch circuit coupled to said plurality of F_ports and said at least one N_port for interconnecting said ports.

10. The switch of claim 9, wherein said at least one N_port operates as a virtual node port, with one virtual node address for each of said plurality of F_ports connected to nodes.

11. The switch of claim 9, wherein said switch circuit is further adapted to act as a firewall.

12. The switch of claim 9, wherein said switch circuit is further adapted for intrusion detection.

13. The switch of claim 9, further comprising:

at least one intermediate port coupled to said switch circuit, wherein said switch circuit routes frames between said plurality of F_ports and said at least one N_port through said at least one intermediate port.

14. The switch of claim 13, wherein the interconnection between said at least one intermediate port and either said plurality of F_ports or said at least one N_port is a private

interconnection and said at least one intermediate port and said other port perform public to private and private to public address translations.

15. The switch of claim 13, wherein the number of intermediate ports equals the number of N_ports.

16. The switch of claim 9, wherein said switch circuit performs public to private and private to public address translations between said plurality of F_ports and said at least one N_port.

17 A network comprising:

a series of nodes;

a first fabric; and

a data switching device connected to said series of nodes and to said first fabric, said device including:

a plurality of fabric ports for connecting to said series of nodes and forming a second fabric;

at least one node port for connecting to said first fabric; and

a switch coupled to said plurality of fabric ports and said at least one node port for interconnecting said ports.

18. The network of claim 17, wherein said at least one node port operates as a virtual node port, with one virtual node address for each of said plurality of fabric ports connected to nodes.

19. The network of claim 17, wherein said switch is further adapted to act as a firewall.

20. The network of claim 17, wherein said switch is further adapted for intrusion detection.

21. The network of claim 17, further comprising:

at least one intermediate port coupled to said switch, wherein said switch routes frames between said plurality of fabric ports and said at least one node port through said at least one intermediate port.

22. The network of claim 21, wherein the interconnection between said at least one intermediate port and either said plurality of fabrics ports or said at least one node port is a private interconnection and said at least one intermediate port and said other port perform public to private and private to public address translations.

23. The network of claim 21, wherein the number of intermediate ports equals the number of node ports.

24. The network of claim 17, wherein said switch performs public to private and private to public address translations between said plurality of fabric ports and said at least one node port.

25. The network of claim 17, wherein said nodes are host computers.

26. The network of claim 25, wherein said host computers are blade computers and are located in a blade server chassis.

27. The network of claim 26, wherein said data switching device is a blade located in said blade server chassis.

28. A network comprising:

a series of nodes;

a first fabric; and

a Fibre channel switch connected to said series of nodes and to said first fabric, said switch including:

a plurality of F_ports for connecting to said series of nodes and forming a second fabric;

at least one N_port for connecting to said first fabric; and

a switch circuit coupled to said plurality of F_ports and said at least one N_port for interconnecting said ports.

29. The network of claim 28, wherein said at least one N_port operates as a virtual node port, with one virtual node address for each of said plurality of F_ports connected to nodes.

30. The network of claim 28, wherein said switch circuit is further adapted to act as a firewall.

31. The network of claim 28, wherein said switch circuit is further adapted for intrusion detection.

32. The network of claim 28, further comprising:

at least one intermediate port coupled to said switch circuit, wherein said switch circuit routes frames between said plurality of F_ports and said at least one N_port through said at least one intermediate port.

33. The network of claim 32, wherein the interconnection between said at least one intermediate port and either said plurality of F_ports or said at least one N_port is a private interconnection and said at least one intermediate port and said other port perform public to private and private to public address translations.

34. The network of claim 32, wherein the number of intermediate ports equals the number of N_ports.

35. The network of claim 28, wherein said switch circuit performs public to private and private to public address translations between said plurality of F_ports and said at least one N_port.

36. The network of claim 28, wherein said nodes are host computers.

37. The network of claim 36, wherein said host computers are blade computers and are located in a blade server chassis.

38. The network of claim 37, wherein said data switching device is a blade located in said blade server chassis.

39. A network comprising:

a series of nodes, each having two ports;

a first fabric; and

two data switching devices, each connected to one port of each of said series of nodes and to said first fabric, each said device including:

a plurality of fabric ports for connecting to said one port of said series of nodes and forming an additional fabric;

at least one node port for connecting to said first fabric; and

a switch coupled to said plurality of fabric ports and said at least one node port for interconnecting said ports.

40. The network of claim 39, wherein said at least one node port operates as a virtual node port, with one virtual node address for each of said plurality of fabric ports connected to nodes.

41. The network of claim 39, wherein said switch is further adapted to act as a firewall.

42. The network of claim 39, wherein said switch is further adapted for intrusion detection.

43. The network of claim 39, further comprising:

at least one intermediate port coupled to said switch, wherein said switch routes frames between said plurality of fabric ports and said at least one node port through said at least one intermediate port.

44. The network of claim 43, wherein the interconnection between said at least one intermediate port and either said plurality of fabrics ports or said at least one node port is a private interconnection and said at least one intermediate port and said other port perform public to private and private to public address translations.

45. The network of claim 43, wherein the number of intermediate ports equals the number of node ports.

46. The network of claim 39, wherein said switch performs public to private and private to public address translations between said plurality of fabric ports and said at least one node port.

47. The network of claim 39, wherein said nodes are host computers.

48. The network of claim 47, wherein said host computers are blade computers and are located in a blade server chassis.

49. The network of claim 48, wherein each said data switching device is a blade located in said blade server chassis.

50. A network comprising:

a series of nodes, each having two ports;

a first fabric; and

two Fibre channel switches connected to one port of each of said series of nodes and to said first fabric, each said switch including:

a plurality of F_ports for connecting to said one port of said series of nodes and forming an additional fabric;

at least one N_port for connecting to said first fabric; and

a switch circuit coupled to said plurality of F_ports and said at least one N_port for interconnecting said ports.

51. The network of claim 50, wherein said at least one N_port operates as a virtual node port, with one virtual node address for each of said plurality of F_ports connected to nodes.

52. The network of claim 50, wherein said switch circuit is further adapted to act as a firewall.

53. The network of claim 50, wherein said switch circuit is further adapted for intrusion detection.

54. The network of claim 50, further comprising:

at least one intermediate port coupled to said switch circuit, wherein said switch circuit routes frames between said plurality of F_ports and said at least one N_port through said at least one intermediate port.

55. The network of claim 54, wherein the interconnection between said at least one intermediate port and either said plurality of F_ports or said at least one N_port is a private interconnection and said at least one intermediate port and said other port perform public to private and private to public address translations.

56. The network of claim 54, wherein the number of intermediate ports equals the number of N_ports.

57. The network of claim 50, wherein said switch circuit performs public to private and private to public address translations between said plurality of F_ports and said at least one N_port.

58. The network of claim 50, wherein said nodes are host computers.

59. The network of claim 58, wherein said host computers are blade computers and are located in a blade server chassis.

60. The network of claim 59, wherein said data switching device is a blade located in said blade server chassis.

61. A network comprising:

a series of nodes, each having two ports;

first and second fabrics; and

two data switching devices, each connected to one port of each of said series of nodes and to said first and second fabrics, each said device including:

a plurality of fabric ports for connecting to said one port of said series of nodes and forming an additional fabric;

two node ports, one for connecting to each of said first and second fabrics; and

a switch coupled to said plurality of fabric ports and said two node ports for interconnecting said ports.

62. The network of claim 61, wherein each of said node ports operates as a virtual node port, with one virtual node address for each of said plurality of fabric ports connected to nodes.

63. The network of claim 61, wherein said switch is further adapted to act as a firewall.

64. The network of claim 61, wherein said switch is further adapted for intrusion detection.

65. The network of claim 61, further comprising:

two intermediate ports coupled to said switch, wherein said switch routes frames between said plurality of fabric ports and said two node ports through one of said intermediate ports.

66. The network of claim 65, wherein the interconnection between each of said intermediate ports and either said plurality of fabrics ports or said node ports is a private interconnection and said intermediate ports and said other ports perform public to private and private to public address translations.

67. The network of claim 61, wherein said switch performs public to private and private to public address translations between said plurality of fabric ports and said node ports.

68. The network of claim 61, wherein said nodes are host computers.

69. The network of claim 68, wherein said host computers are blade computers and are located in a blade server chassis.

70. The network of claim 69, wherein each said data switching device is a blade located in said blade server chassis.

71. A network comprising:

a series of nodes, each having two ports;

first and second fabrics; and

two Fibre channel switches connected to one port of each of said series of nodes and to said first and second fabrics, each said switch including:

a plurality of F_ports for connecting to said one port of said series of nodes and forming an additional fabric;

two N_ports, one for connecting to each of said first and second fabrics; and

a switch circuit coupled to said plurality of F_ports and said two N_ports for interconnecting said ports.

72. The network of claim 71, wherein each of said N_ports operates as a virtual node port, with one virtual node address for each of said plurality of F_ports connected to nodes.

73. The network of claim 71, wherein said switch circuit is further adapted to act as a firewall.

74. The network of claim 71, wherein said switch circuit is further adapted for intrusion detection.

75. The network of claim 71, further comprising:

two intermediate ports coupled to said switch circuit, wherein said switch circuit routes frames between said plurality of F_ports and said two N_ports through one of said two intermediate ports.

76. The network of claim 75, wherein the interconnection between each of said intermediate ports and either said plurality of F_ports or said N_ports is a private interconnection and said intermediate ports and said other ports perform public to private and private to public address translations.

77. The network of claim 71, wherein said switch circuit performs public to private and private to public address translations between said plurality of F_ports and said N_ports.

78. The network of claim 71, wherein said nodes are host computers.

79. The network of claim 78, wherein said host computers are blade computers and are located in a blade server chassis.

80. The network of claim 79, wherein said data switching device is a blade located in said blade server chassis.

81. A network comprising:

a series of nodes, each having two ports;

first and second fabrics; and

two data switching devices, each connected to one port of each of said series of nodes and to one of said first and second fabrics, each said device including:

a plurality of fabric ports for connecting to said one port of said series of nodes and forming an additional fabric;

two node ports for connecting to one of said first and second fabrics; and

a switch coupled to said plurality of fabric ports and said two node ports for interconnecting said ports.

82. The network of claim 81, wherein each of said node ports operates as a virtual node port, with one virtual node address for each of said plurality of fabric ports connected to nodes.

83. The network of claim 81, wherein said switch is further adapted to act as a firewall.

84. The network of claim 81, wherein said switch is further adapted for intrusion detection.

85. The network of claim 81, further comprising:

two intermediate ports coupled to said switch, wherein said switch routes frames between said plurality of fabric ports and said two node ports through one of said intermediate ports.

86. The network of claim 85, wherein the interconnection between each of said intermediate ports and either said plurality of fabrics ports or said node ports is a private interconnection and said intermediate ports and said other ports perform public to private and private to public address translations.

87. The network of claim 81, wherein said switch performs public to private and private to public address translations between said plurality of fabric ports and said node ports.

88. The network of claim 81, wherein said nodes are host computers.

89. The network of claim 88, wherein said host computers are blade computers and are located in a blade server chassis.

90. The network of claim 89, wherein each said data switching device is a blade located in said blade server chassis.

91. A network comprising:

a series of nodes, each having two ports;

first and second fabrics; and

two Fibre channel switches connected to one port of each of said series of nodes and to one of said first and second fabrics, each said switch including:

a plurality of F_ports for connecting to said one port of said series of nodes and forming an additional fabric;

two N_ports for connecting to one of said first and second fabrics; and

a switch circuit coupled to said plurality of F_ports and said two N_ports for interconnecting said ports.

92. The network of claim 91, wherein each of said N_ports operates as a virtual node port, with one virtual node address for each of said plurality of F_ports connected to nodes.

93. The network of claim 91, wherein said switch circuit is further adapted to act as a firewall.

94. The network of claim 91, wherein said switch circuit is further adapted for intrusion detection.

95. The network of claim 91, further comprising:

two intermediate ports coupled to said switch circuit, wherein said switch circuit routes frames between said plurality of F_ports and said two N_ports through one of said two intermediate ports.

96. The network of claim 95, wherein the interconnection between each of said intermediate ports and either said plurality of F_ports or said N_ports is a private interconnection and said intermediate ports and said other ports perform public to private and private to public address translations.

97. The network of claim 91, wherein said switch circuit performs public to private and private to public address translations between said plurality of F_ports and said N_ports.

98. The network of claim 91, wherein said nodes are host computers.

99. The network of claim 98, wherein said host computers are blade computers and are located in a blade server chassis.

100. The network of claim 99, wherein said data switching device is a blade located in said blade server chassis.

101. A method for routing between a series of nodes and a first fabric using a data switching device, the method comprising:

providing a plurality of fabric ports on the device for connecting to the series of nodes and forming a second fabric;

providing at least one node port on the device for connecting to the first fabric; and

interconnecting said plurality of fabric ports and said at least one node port with the device.

102. The method of claim 101, further comprising operating said at least one node port as a virtual node port, with one virtual node address for each of said plurality of fabric ports connected to nodes.

103. The method of claim 101, further comprising:

routing frames between said plurality of fabric ports and said at least one node port through at least one intermediate port on the device.

104. The method of claim 103, wherein the interconnection between said at least one intermediate port and either said plurality of fabrics ports or said at least one node port is a private interconnection and said at least one intermediate port and said other port perform public to private and private to public address translations.

105. The method of claim 103, wherein the number of intermediate ports equals the number of node ports.

106. The device of claim 101, further comprising performing public to private and private to public address translations between said plurality of fabric ports and said at least one node port.